IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW HAMPSHIRE

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH TRAVELAGENT613@YAHOO.COM THAT IS STORED AT PREMISES CONTROLLED BY OATH HOLDINGS, INC.	Case No. 19-mj-23-01-AJ **Filed Under Seal**

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Special Agent John Chamberlain, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with a certain account that is stored at premises controlled by Oath Holdings, Inc., an email provider headquartered at 701 First Avenue, Sunnyvale, California. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Oath Holdings, Inc. to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I am currently employed as the Assistant Federal Security Director—Law Enforcement (AFSD-LE) with the Department of Homeland Security, Transportation Security

Administration ("DHS/TSA"), Office of Inspection ("OOI") with the Federal Air Marshal Service.

3. I have been an AFSD-LE with the DHS/TSA since July of 2018. Prior to this assignment, I was detailed as a Special Agent to the TSA Office of Investigations from 2011 through 2018. I have been a Federal Air Marshal for the United States for approximately 27 years, and in that capacity have served as an Assistant Special Agent in Charge from 2001 to 2007 and as Special Agent in Charge from 2007 to 2011 in the Boston Federal Air Marshal Field Office. Prior to September 11, 2001, I was assigned as a Supervisor or Assistant Supervisor for the Federal Air Marshals, and in that capacity led Federal Air Marshal teams on counterterrorist missions domestically and internationally from 1991 through 2001. I have been assigned to various locations and investigative responsibilities in New Jersey, and Massachusetts.

4. Prior to joining the Federal Air Marshal Service, I was a Criminal Investigator, Special Agent, with the United States Army Criminal Investigation Division from 1989-1991. In that capacity, I served as a criminal investigator charged with enforcing all laws associated with the United States Military Uniform Code of Military Justice, and served in both the United States and Republic of South Korea.

5. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

6. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of Title 18, United States Code, Sections 1028 and 1029 (identity theft and access device fraud) have been committed by Hayder Lefta ("LEFTA"). There is also probable cause to search the information described in Attachment A

for evidence, instrumentalities, contraband, and/or fruits of these crimes further described in Attachment B.

JURISDICTION

7. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

PROBABLE CAUSE

8. In December of 2018, the Londonderry Police Department received a report from S.O. about fraudulent purchases made on his credit card. S.O. flew out of the Manchester Boston Regional Airport on September 17, 2018, where he used his credit card to pay for baggage at the United Airlines ticket counter and a meal at Burger King. S.O. recalled that when he paid for baggage, the United Airlines Customer Service Representative took his card behind the counter and out of sight. He recalled that the Burger King employee never took the credit card and he paid by placing the card's chip in a machine.

9. S.O.'s bank notified him that there were suspicious charges on his account on September 19, 2018, and September 20, 2018, shortly after he flew out of Manchester. S.O. confirmed that these were unauthorized charges. The unauthorized charges that were processed included $112.31 at Domino's Pizza in Manchester and two charges used to purchase tickets on Turkish Airlines, in the amounts of $2,657.13 and $1,488.91.[1]

[1] There were additional attempted purchases on the credit card that were reportedly not made by S.O. including at Zoro Tools Inc., Kennedy Fried Chicken in Manchester, New Hampshire, and T-Mobile.

10. Investigators determined, based on United Airlines records, that LEFTA was the United customer service representative who processed S.O.'s baggage fee payment at the Manchester Airport on September 17, 2018.

11. Investigators contacted the Domino's Pizza where the credit card was used and received records of the transaction. The Domino's invoice indicated that an order for delivery to United Airlines at the Manchester, New Hampshire, airport was placed on September 19, 2018. The phone number listed on the order was (786) 562-4605 ("the 4605 Phone").[2] The signature on the credit card slip is illegible. Officers interviewed the delivery driver who said that he remembered delivering pizzas to the airport that day (because the airport was out of his normal delivery area and he rarely delivered there). He described the person he met as a "skinny" male approximately 5'8 to 5'10 and 165 pounds, of Middle Eastern descent. This description is consistent with LEFTA. Investigators determined that LEFTA was working at the time of the pizza delivery.

12. Investigators issued a subpoena to Turkish Airlines for information about the flights purchased with S.O.'s credit card. Information from Turkish Airlines indicated that tickets were purchased for three individuals, Qassam Raheeah, Saef Rabeah, and Fazza Mohammad on September 18, 2018. On September 20, 2018, a ticket was purchased for Andy Ibraham. The email address associated with the purchases is Travelagent613@yahoo.com and the phone number is the 4605 Phone. Investigators are not aware of any association between LEFTA and Raheeah, Rabeah or Mohammed. However, United Airlines records show that LEFTA and

[2] Although I have not received subscriber information from this number, a reliable law enforcement database associates it with Karar Lefta. Other than having the same last name, I do not know if or how this person is associated with LEFTA.

Ibraham have traveled together in the past. On October 8, 2018, an individual appeared in person at the Turkish Airlines facility in Boston to change three of these reservations. The change fee for the tickets was paid for with a credit card in LEFTA's name.

13. United Airlines confirmed that the email address Travelagent613@yahoo.com had been used on travel reservations made by LEFTA for his own person travel in the past. United Airlines records show a different telephone number, (207) 385-7762 as the contact number for LEFTA (and a third number with a 515 area code was associated with him in the past).

14. Investigators working at the Manchester airport have observed LEFTA carrying at least two cellular telephones. On January 23, 2018, a law enforcement officer placed a call to the 4605 Phone while surveilling LEFTA and observed LEFTA answer the phone.

15. I conducted research into LEFTA's travel history and learned that in November 7, 2017, Customs and Border Protection ("CBP") conducted a secondary screening on LEFTA when he entered the United States by car through the Mexican border. He possessed what appeared to be $1,500 of novelty money and a credit card in someone else's name. During that screening, LEFTA possessed two iPhones (an iPhone 6+ and an iPhone 8+). The iPhone 6 had the 4605 Phone number associated with it. During the secondary inspection, CBP officers looked through the phones and noticed that there was a significant amount of personal information of various individuals that appeared to be taken from United Airlines databases. LEFTA told officers that he collected the information to keep in contact with people on social media. When asked about why he had the credit card, he said that the owner was his friend, but did not know how it ended up in his possession. During this encounter, LEFTA provided agents with three email addresses, none of which were the travelagent613@yahoo.com account referenced here.

Officers searching his phone found ten additional email addresses apparently accessed from the phone, one of which was travelagent613@yahoo.com.

16. On January 28, 2019, LEFTA was arrested by the Londonderry Police Department during his shift at the Manchester airport on state charges related to the fraudulent use of a credit card, identity fraud, theft by deception, and forgery. He was read his *Miranda* rights. At the time of his arrest, LEFTA had been working at the ticket counter desk. On the desk were the three iPhones and the iPad. Investigators asked LEFTA about the iPhones. He said that one of them was the 4605 number.

17. After observing the arrest, another employee opened LEFTA's backpack and showed officers a computer inside. An officer seized the computer. LEFTA was asked about the computer and confirmed that it was his. Investigators received a warrant to search the iPhones, iPad, and computer. The forensic examination of the devices is ongoing but a preliminary review indicates that some evidence of the travelagent613@yahoo.com account has been found on at least one of the devices. As this email address was used to book airline tickets with S.O.'s credit card, as LEFTA has used it to book his own travel in the past, and as I believe he has collected personally identifiable information from United Airlines records in the past, I believe that evidence of the criminal violations discussed herein will be found on the email account. I also know that email accounts often maintain records of purchases, travel, financial transactions, and communications with co-conspirators.

18. On January 18, 2019, Oath Holdings, Inc. was served with a preservation letter under 18 U.S.C. § 2703(f) related to the Travelagent613@yahoo.com account.

BACKGROUND CONCERNING EMAIL

19. In my training and experience, I have learned that Oath Holdings, Inc. provides a variety of on-line services, including electronic mail ("email") access, to the public. Oath Holdings, Inc. allows subscribers to obtain email accounts at the domain name yahoo.com like the email account listed in Attachment A. Subscribers obtain an account by registering with Oath Holdings, Inc., which provides Yahoo email addresses (hereinafter referred to as Yahoo). During the registration process, Yahoo asks subscribers to provide basic personal information. Therefore, the computers of Oath Holdings, Inc. are likely to contain stored electronic communications (including retrieved and unretrieved email for Yahoo subscribers) and information concerning subscribers and their use of Yahoo's services, such as account access information, email transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

20. A Yahoo subscriber can also store with the provider files in addition to emails, such as address books, contact or buddy lists, calendar data, pictures (other than ones attached to emails), and other files, on servers maintained and/or owned by Oath Holdings, Inc. In my training and experience, evidence of who was using an email account may be found in address books, contact or buddy lists, email in the account, and attachments to emails, including pictures and files.

21. In my training and experience, email providers generally ask their subscribers to provide certain personal identifying information when registering for an email account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such

information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and my experience, I know that, even if subscribers insert false information to conceal their identity, this information often provides clues to their identity, location, or illicit activities.

22. In my training and experience, email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (*i.e.*, session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, email providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.

23. In my training and experience, in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

24. Based on my training and experience, I know that Yahoo maintains records that can link different Yahoo accounts to one another, by virtue of common identifiers, such as common e-mail addresses, common telephone numbers, common device identifiers, common computer cookies, and common names or addresses, that can show a single person, or single group of persons, used multiple Yahoo/Oath Holdings, Inc. accounts. Based on my training and experience, I also know that evidence concerning the identity of such linked accounts can be useful evidence in identifying the person or persons who have used a particular Yahoo account.

25. As explained herein, information stored in connection with an email account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, email communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the email provider can show how and when the account was accessed or used. For example, as described below, email providers typically log the Internet Protocol (IP) addresses from which users access the email account, along with the time and date of that access. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculpate or exculpate the account owner. Additionally,

information stored at the user's account may further indicate the geographic location of the account user at a particular time (*e.g.*, location information integrated into an image or video sent via email). Last, stored electronic data may provide relevant insight into the email account owner's state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner's motive and intent to commit a crime (*e.g.*, communications relating to the crime), or consciousness of guilt (*e.g.*, deleting communications in an effort to conceal them from law enforcement).

CONCLUSION

26. Based on the forgoing, I request that the Court issue the proposed search warrant. Because the warrant will be served on Oath Holdings, Inc. who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

Respectfully submitted,

/s/ John Chamberlain
John Chamberlain
Special Agent
Homeland Security Investigations, TSA

Subscribed and sworn to before me on February 5, 2019

Honorable Andrea K. Johnstone
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with TravelAgent613@Yahoo.com that is stored at premises owned, maintained, controlled, or operated by Oath Holdings, Inc., a company headquartered at 71 First Avenue, Sunnyvale, California, 94089.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Oath Holdings, Inc. (the "Provider")

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f) on January 18, 2019, the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. The contents of all emails associated with the account from November 7, 2017, to January 28, 2019, including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;

b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

c. The types of service utilized;

d. All records or other information stored by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files; other linked accounts; and

e. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken.

The Provider is hereby ordered to disclose the above information to the government within **14 days** of service of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence, and instrumentalities of violations of Title 18, United States Code, Sections 1028 and 1029 (identity theft and access device fraud), those violations involving **Hayder Lefta** and occurring between November 17, 2017 and January 28, 2019 including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

(a) Information that constitutes evidence concerning identity theft and access device fraud including: personally identifiable information (PII) of third parties and credit card or banking information; documents (including notes, emails, photographs, or communications) relating to unauthorized access of the United Airlines systems to collect PII and/or other information about passengers; information about any purchases by LEFTA or others (including those made on LEFTA's credit card or credit cards belonging to others) including records, receipts, notes, ledgers, bank account information, and other financial documentation; and receipts, tickets, notes and other records relating to domestic and international travel.

(b) Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;

(c) Evidence indicating the email account owner's state of mind as it relates to the crime under investigation;

(d) The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s); and

(e) Information that constitutes evidence concerning persons who either (i) collaborated, conspired, or assisted (knowingly or unknowingly) the commission of the criminal activity under investigation; or (ii) communicated with the Account about matters relating to the criminal activity under investigation, including records that help reveal their whereabouts.

CERTIFICATE OF AUTHENTICITY OF DOMESTIC RECORDS PURSUANT TO FEDERAL RULES OF EVIDENCE 902(11) AND 902(13)

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by Oath Holdings, Inc., and my title is _____. I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of Oath Holdings, Inc. The attached records consist of _____ **[GENERALLY DESCRIBE RECORDS (pages/CDs/megabytes)]**. I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of Oath Holdings, Inc., and they were made by Oath Holdings, Inc. as a regular practice; and

b. such records were generated by Oath Holdings, Inc.'s electronic process or system that produces an accurate result, to wit:

1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of Oath Holdings, Inc. in a manner to ensure that they are true duplicates of the original records; and

2. the process or system is regularly verified by Oath Holdings, Inc., and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

Date	Signature